Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Advanced Methods to Target and Eliminate Unlawful Robocalls	)	CG Docket No. 17-59
	)	
Call Authentication Trust Anchor		WC Docket No. 17-97

COMMENTS OF ICONECTIV

iconectiv welcomes the opportunity to submit these comments on the Federal Communications Commission's ("FCC" or "Commission") Further Notice of Proposed Rulemaking in the above-referenced proceeding ("Further Notice")[1], in which the Commission seeks comment on proposed rules that will help to eliminate illegal robocalls that originate abroad by placing new obligations on the gateway providers that are the point of entry for foreign calls into the United States, requiring them to lend a hand in the fight against illegal robocalls originating abroad.

I. INTRODUCTION

As a neutral and trusted partner to the industry, iconectiv has been a longstanding and active participant in the ATIS / SIP Forum IP NNI taskforce working to define a call authentication framework as part of the toolkit to mitigate illegal robocalls. In addition to contributing substantial foundational work for the SHAKEN framework, iconectiv has been a prime contributor on the governance and certificate management aspects of SHAKEN and has served as the Policy Administrator for the Call Authentication Trust Anchor since 2019.

As administrator of the industry-backed Registered Caller™ solution for enterprise attestation, in partnership with CTIA, iconectiv continues to work with government and industry stakeholders on solutions to address the needs of the more complex call topologies and telephone number relationships that are not fully addressed within the initial STIR/SHAKEN framework. The iconectiv comments that follow primarily focus on technical and operational considerations related to Know Your Customer (KYC) requirements and the challenges associated with the multiple hop call topologies that are commonplace with cross-border traffic. iconectiv's input should not be considered a recommendation for Commission action.

II. COMMENTS

[1] Targeting Gateway Providers to Combat Illegal Robocalls, Further Notice of Proposed Rulemaking, CG Docket No. 17-59; WC Dockett No. 17-97, FCC 21-105, (rel. Oct. 1, 2021) ("Further Notice").

45. The FCC seeks comment on whether to limit gateway providers to assigning a certain attestation level or levels, and if so what level? Under what circumstances would gateway providers be able to assign, and anticipate assigning, an A- or B-level attestation?[2]

iconectiv suggests there is no reason to arbitrarily limit the attestation level that a gateway provider can use when authenticating a call given the requirement to comply with the relevant standards. A gateway provider who has established reliable mechanisms with their upstream partners that clearly indicate which traffic is attestation level A, B, or C should be permitted to transmit that attestation downstream in order to be available to the terminating provider. Harmonization of the call authentication requirements across intermediate providers, originating and terminating providers was established in the *Second Caller ID Authentication Report and Order* [3] where the Commission already allows U.S. call originations that are authenticated by an intermediate provider to use any of the attestation levels, if consistent with industry standards. This harmonization could also apply to gateway providers handling foreign call originations to further encourage industry progress in resolving the challenges with mitigating illegal robocalls from overseas.[4] The Commission also acknowledges in various sections of this Further Notice,[5] that call authentication may accompany foreign originations. Accordingly, this rulemaking should not preclude gateway providers transmitting cross-border call authentication received from foreign voice service providers or, where call authentication is not present, adding attestation information in a manner consistent with industry standards.

46. *Non-IP Network Technology.* The FCC seeks comment whether they should mandate that gateway providers with non-IP network technology implement a non-IP caller ID authentication solution, such as Out-of-Band STIR?[6]

iconectiv would like to clarify to the Commission that they have referred to Out-of-Band STIR without reference to Out-of-Band SHAKEN, the latter defining critical governance and management requirements that ensure integrity in the framework when relying on Out-of-Band technology. In reference to the question, iconectiv understands that there is a significant amount of TDM interconnection used in cross-border calls and support of Out-of-Band STIR/SHAKEN by the gateway provider would enable authentication of this large volume of calls and not require SIP-based U.S. service providers to invest in additional call authentication for legacy technologies.[7]

80. The Commission proposes and seeks comment on requiring gateway providers to confirm that a foreign call originator is authorized to use a particular U.S. number that purports to originate the call.[8]

---

[2] See Further Notice ¶ 45

[3] Call Authentication Trust Anchor, WC Docket No. 17-97, Second Report and Order, 36 FCC Rcd 1859, 1926-1927, ¶ 142 (2020) (Second Caller ID Authentication Report and Order).

[4] Second Caller ID Authentication Report and Order, 36 FCC Rcd, 1927, ¶ 143

[5] See Further Notice ¶ ¶ 22, 43, 69

[6] See Further Notice ¶ 46

[7] ATIS-1000096, Signature-based Handling of Asserted information using toKENs (SHAKEN): Out-of-Band PASSporT Transmission Involving TDM Networks p. 1

[8] See Further Notice ¶ 80

The Commission correctly notes the gateway provider usually has no direct relationship with the call originator. Indeed, iconectiv understands the gateway provider is often multiple hops away from that originator making such a requirement extremely challenging. Furthermore, selection of the gateway provider may vary with each call and is affected by factors such as least cost routing and quality of service. iconectiv believes this complexity would make it cost prohibitive for gateway providers to maintain accurate data regarding all possible foreign call originators and which U.S. numbers they are authorized to use. Even with all that effort, absent call authentication upstream, a fraudster could still spoof these U.S. numbers and be undetectable if located multiple hops away from the gateway provider. Traceback is valuable when callers spoof, and quick action can be especially beneficial. However manual efforts are often required to trace as far back as the originating foreign service provider who has the relationship with the call originator. Absent attestation information from the STIR/SHAKEN framework, there is no scalable way to identify a call's true source in the presence of multiple hops behind the gateway provider. For similar reasons, within the U.S. which also has significant multi-hop traffic, intermediate providers are not required to confirm a call originator is authorized to use a particular U.S. number. This issue was addressed by requiring originating voice service providers to authenticate their calls in a manner that can be conveyed to the terminating service provider securely. This was one of the key reasons to require originating service providers to use STIR/SHAKEN and can also be effective with global traffic when complemented with appropriate trust policies, traceback processes, and call blocking rules.

82, 85. The Commission also seeks comment on whether there is the possibility for gateway providers to have contractual relationships with call originators, distinct from their position on the call path, such that they will transmit all calls for a particular caller.[9] Further, the Commission asks whether they should consider the call originator the gateway provider's "customer" for purposes of KYC requirements.[10]

iconectiv understands that traffic paths between a foreign originator and the U.S. are highly dynamic, often multi-hop, and depend on congestion levels, balance of trade requirements, costs, etc. Therefore, a gateway provider is very unlikely to have a contractual or customer relationship covering all calls from foreign service providers or foreign call originators. Absent call authentication, which would clearly identify the originator, it would also be very challenging to know which originator contract applies to any traffic not directly connected to a gateway provider.

88. The Commissions asks, "Are we correct in anticipating that if a foreign partner cannot validate the number, there is a significant risk that the number is being spoofed and is therefore likely to be involved in an illegal robocalling campaign?"[11]

iconectiv does not believe such a conclusion can be drawn given the prevalence of commercial callers originating with third party numbers as the caller ID. For domestic calls using third party

[9] See Further Notice ¶ 82
[10] See Further Notice ¶ 85
[11] See Further Notice ¶ 88

numbers,[12] additional mechanisms have been found to be necessary to validate an originator's authority to use a U.S. number. The same should be expected of foreign call originations.

III. CONCLUSION

Multi-hop call topologies typical of foreign originations drive significant complexities related to gateway providers establishing contracts and fulfilling KYC requirements with call originators. Caller ID authentication by originating foreign voice service providers is the only scalable way to identify a call's true source. iconectiv believes the Commission's efforts to address the illegal robocalls coming from cross-border traffic should allow all providers to support caller ID authentication from originating foreign voice service providers to address the global spoofing problem at scale.

iconectiv appreciates the opportunity to provide its input to the Further Notice of Proposed Rulemaking for consideration in determining the outcome of this docket.

Respectfully submitted,

/s/ Chris Drake
Chris Drake
Chief Technology Officer
iconectiv, LLC
100 Somerset Corporate Blvd.
Bridgewater, NJ 08807
(732)699-2035
cdrake@iconectiv.com

December 10, 2021

[12] ATIS-1000089.v002, Study of Full Attestation Alternatives for Enterprises and Business Entities with Multi-Homing and Other Arrangements (May 2021)